METHODS, SYSTEMS AND COMPUTER PROGRAM PRODUCTS FOR GENERATING USER-DEPENDENT RSA VALUES WITHOUT STORING SEEDS

Abstract of the Disclosure

Methods, systems and computer program products are provided which allow for generation and authentication of RSA encrypted values by utilizing a combination of entity specific information such as biometric information and by incorporating information about the secret seeds into the cryptographic values p and q utilized to encrypt the information. Thus, authentication of an encrypted message may be achieved without requiring storage of the secret seed values utilized to generate the cryptographic values. Furthermore the present invention assures that users with different entity specific information utilize different p and q values.